IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Atsushi Fujioka et al.

Serial No. To be assigned — Art Unit: To be assigned

Filed: Herewith — Examiner: To be assigned

For: ELECTRONIC VOTING METHOD AND SYSTEM AND RECORDING MEDIUM HAVING RECORDED THEREON A PROGRAM FOR IMPLEMENTING THE METHOD — Atty Docket: 162/534

SUBMISSION OF CERTIFIED PRIORITY DOCUMENT(S) and CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Priority under 35 U.S.C. § 119 is hereby claimed to the following priority document(s), certified copies of which are enclosed. The documents were filed in a foreign country within the proper statutory period prior to the filing of the above-referenced United States patent application.

Country	Priority Document Serial No.	Filing Date
Japan	10-320173	November 11, 1998

Acknowledgement of this claim and submission in the next official communication is respectfully requested.

Respectfully submitted,

Morris Liss, Reg. No. 24,510
Pollock, Vande Sande & Amernick, R.L.L.P.
1990 M Street, N.W.
Washington, D. C. 20036-3425
Telephone: 202-331-7111

Date: 11/5/99

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年１１月１１日

出願番号
Application Number: 平成１０年特許願第３２０１７３号

出願人
Applicant (s): 日本電信電話株式会社

１９９９年 ８月１６日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０５７２５２

【書類名】　特許願

【整理番号】　NTTH106401

【提出日】　平成10年11月11日

【あて先】　特許庁長官殿

【国際特許分類】　G07C

【発明の名称】　電子投票方法、装置及びプログラム記録媒体

【請求項の数】　6

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　藤岡　淳

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　阿部　正幸

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　三浦　史光

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100066153

【弁理士】

【氏名又は名称】　草野　卓

【選任した代理人】

【識別番号】　100100642

【弁理士】

【氏名又は名称】　稲垣　稔

【手数料の表示】

【予納台帳番号】　002897

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　電子投票方法、装置及びプログラム記録媒体

【特許請求の範囲】

【請求項１】　投票者は、投票内容を暗号化器を用いて暗号化し、その暗号化投票内容を、乱数発生器を用いて生成した乱数成分とともに撹乱器に入力して撹乱された投票文を作成し、この投票文を選挙管理者装置に送信し、

選挙管理者は、投票者の確認を行った後に、受信した投票文を署名作成器に入力して投票文の署名を生成し、これを投票者装置に送り返し、

投票者は、受信した投票文の署名を乱数成分除去器に入力し、乱数成分の影響を取り除いて暗号化投票内容の署名情報を求め、その署名情報と上記暗号化投票内容装置へ送信し、

集計者は、暗号化投票内容と受信した署名情報を署名検査器に入力して投票文が選挙管理者によって署名されていることを確認し、暗号化投票内容を表にしてこれを周知し、

投票者は、自分の暗号化投票内容が表に存在することを確認し、

集計者は、復号器を用いて暗号化投票内容を復号して開票を行う電子投票方法。

【請求項２】　集計者とその装置を複数置き、それぞれが備える復号器を用いて開票を行うことを特徴とする請求項１記載の電子投票方法。

【請求項３】　複数ある復号器の中の一定数のものだけを用いて開票を行えることを特徴とする請求項２記載の電子投票方法。

【請求項４】　投票者装置と、選挙管理者装置及び集計者装置とがそれぞれ通信路で接続され、

投票者装置は、

投票内容を集計者装置の暗号化鍵で暗号化する暗号化器と、

乱数を発生する乱数発生器と、

上記暗号化投票内容と上記乱数を撹乱して投票文を作成する撹乱器と、

上記投票文の署名を生成する署名作成器と、

上記投票文及びその署名を選挙管理者装置へ送信する手段と、

選挙管理者装置から受信した投票文署名から乱数成分の影響を取り除いて暗号化投票内容の署名情報を求める乱数成分除去器と、

上記暗号化投票内容の署名情報を検証する署名検査器と、

その署名検査器の検証に合格すると上記暗号化投票内容署名情報及び上記暗号化投票内容を集計者装置へ送信する手段と、

集計者装置から受信した投票内容一覧表に自己の暗号化投票内容が存在するか否かを検査する検査器とを備え、

選挙管理者装置は、

投票者装置から受信した投票文及びその署名を検証する署名検査器と、

その検証に合格すると、上記受信した投票文を入力して投票文の署名を生成する署名作成器と、

上記投票文の署名を投票者装置へ送信する手段とを備え、

集計者装置は、

投票者装置から受信した暗号化投票内容と暗号化投票内容の署名情報を入力して署名を検証する署名検査器と、

その検証に合格すると各投票者装置から受信した暗号化投票内容の表を作成する表作成器と、

暗号化投票内容を復号して開票する復号器とを備える

ことを特徴とする電子投票システム。

【請求項５】　電子投票システムに用いられる投票者装置であって、

投票内容を集計者装置の暗号化鍵で暗号化する暗号化器と、

乱数を発生する乱数発生器と、

上記暗号化投票内容と上記乱数を撹乱して投票文を作成する撹乱器と、

上記投票文の署名を生成する署名作成器と、

上記投票文及びその署名を選挙管理者装置へ送信する手段と、

選挙管理者装置から受信した投票文署名と上記乱数を入力して投票文署名から乱数成分の影響を取り除いて暗号化投票内容の署名情報を求める乱数成分除去器と、

上記暗号化投票内容の署名情報と上記暗号化投票内容を入力して、上記暗号化

投票内容の署名情報を検証する署名検査器と、

その署名検査器の検証に合格すると上記暗号化投票内容の署名情報及び上記暗号化投票内容を集計者装置へ送信する手段と、

集計者装置から受信した投票内容一覧表に自己の暗号化投票内容が存在するか否かを検査する検査器とを備える投票者装置。

【請求項６】　電子投票システムの投票者装置のコンピュータが実行するプログラムを記録した記録媒体であって、

投票内容を集計者装置の暗号化鍵で暗号化する処理と、

乱数を発生する処理と、

上記暗号化投票内容と上記乱数を撹乱して投票文を作成する処理と、

上記投票文の署名を生成する処理と、

上記投票文及びその署名を選挙管理者装置へ送信する処理と、

上記乱数を用いて、選挙管理者装置から受信した投票文署名から乱数成分の影響を取り除いて暗号化投票内容の署名情報を求める処理と、

上記暗号化投票内容を用いて、上記暗号化投票内容の署名情報を検証する処理と、

その検証に合格すると上記暗号化投票内容署名情報及び上記暗号化投票内容を集計者装置へ送信する処理と、

集計者装置から受信した投票内容一覧表に自己の暗号化投票内容が存在するか否かを検査する処理とを

上記コンピュータが実行するプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、電気通信システムでアンケート調査等を行う場合に、安全で、かつ、公平な無記名投票を実現しようとする電子投票システム、投票方法及びプログラム記録媒体に関する。

【０００２】

【従来の技術】

無記名投票は、投票者と投票内容の対応を秘密にでき、個人の思想信条に関するプライバシーを守るのに適しているので、電子会議やＣＡＴＶ等の双方向通信でのアンケート調査等に利用できる。

電気通信において、安全で、かつ、公平な無記名投票を行うには、投票者の偽装や二重投票、投票文の盗聴に伴う投票内容の漏洩等の防止が必要である。これらの問題を解決する方法として、ディジタル署名を用いた電子投票方式が提案されており、例えば、Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta: “A practical secret voting scheme for large scale elections”, in Advances in Cryptology-AUSCRYPT'92, Lecture Notes in Computer Science 718, Springer-Verlag, Berlin, pp.244-251(1993)、特願平４－１７０８９９号「電子投票方法および装置」がある。

【０００３】

しかしながら、この方法には、いくつかの欠点が存在する。

まず、投票者が投票締切後に自分の投票を確認し、再度復号化鍵を集計者に送信することが必要であり、すなわち、投票者の利便性の低いシステムである。

また、集計者は単独であり、耐故障性の低いシステムである。

【０００４】

【発明が解決しようとする課題】

この発明の目的は、プライバシーを侵すことなく異議申し立てが行え、集計の途中経過が投票に影響を与えず、また、集計者の不正や機能不全に対処できる、安全、公平、かつ、簡便な電子投票システム及びその方法を構築することにある。

【０００５】

【課題を解決するための手段】

この発明では、投票者が投票内容を集計者の暗号化鍵で暗号化し、さらにその暗号化投票内容を乱数で撹乱して投票文を作成して、その投票文に署名を付けて選挙管理者に送信する。選挙管理者は、付加された署名を用いて投票者の正当性を認証した後に、投票文に署名して投票文の署名を各投票者に送り返す。投票者は投票文の署名から乱数の影響を取り除いて投票文の署名情報を求め、集計者に

送信する。集計者は受信した投票文の署名情報が選挙管理者によって署名されていることを確認した後に、投票文を暗号化されたまま公開する。それぞれの投票者が、公開された投票文の一覧表に自分の投票文が登録されていることを確認した後に、集計者は、自らが保持する復号化鍵を用いて投票文からすべての投票内容を取り出し、これを集計する。もし、登録されていない場合には、集計者に対して異議を申し立てる。また、集計者を複数とし、それぞれが復号化鍵の一部を保持し、集計者全員もしくは一定数が協力することによって、投票文からすべての投票内容を取り出すこともできるとする。

【０００６】

まず、投票文は投票内容を乱数で撹乱しているので、選挙管理者、および集計者は、撹乱された投票文から投票内容を求めることが出来ず、投票の無記名性が保障できる。

ここで、復号化鍵は集計者が保持しており、投票者は、開票のために再度集計者へ通信を行なう必要がない。

【０００７】

以上より、この発明では、従来より指摘されていた投票者の利便性の問題を解決できる。

次に、集計者を複数とし、それらが協力することにより暗号化された投票文を開票する場合は、異議申し立て時に、自分が正当な投票者であることは、暗号化されている投票文と選挙管理者の署名を送るだけで示すことができる。すなわち、複数存在する集計者の一部に不正者が存在したとしても、全員もしくは一定数の集計者が協力しないかぎり投票内容が明らかになることはない。

【０００８】

また、分散された集計者には、暗号化された投票内容が集まるので、この場合も全員もしくは一定数の集計者が協力しないかぎり、投票の間にその途中経過は明らかにならないので、公平な投票方式となっている。

さらに、集計者全員でなく一定数が協力するだけで開票が可能な場合は、集計者内の何人かが不正者、もしくは、開票への協力が不可能となっても、正しく開票作業を行なうことができるので、この方式は耐故障性の高いシステムであると

言える。

【０００９】

【発明の実施の形態】

以下に、この発明の第一の実施例について説明する。

図１ａはこの発明の全体構成を示す図である。Ｔ人の投票者の装置（投票者装置）１００は、選挙管理者の装置（選挙管理者装置）２００と、また集計者の装置（集計者装置）３００と、それぞれ記名通信路４００、および匿名通信路５００を介して結合されている。また、集計者は投票内容の一覧表６００を公開し、投票者は全員、これにアクセスが可能であるとする。図２にこの発明の投票システムにおける通信シーケンス例を示し、以下、それぞれ、図３に投票者装置１００の構成例を、図４に選挙管理者装置３００の構成例を、図５に集計者装置４００の構成例を示す。また、図１ｂに投票後の投票内容の一覧表を、図１ｃに集計後の投票内容の一覧表を例示する。

【００１０】

以下では、特に投票者V_iが投票内容v_iを選挙管理者Ａの承認を得た後に、集計者Ｃに対して投票する場合について説明する。

ここで、簡単のため、以下のような記法を用いる。

$x=\xi_C(v)$：集計者Ｃの暗号化関数（ｖ：メッセージ）

$v=\rho_C(x)$：集計者Ｃの復号化関数（ｘ：暗号文）

$s=\sigma_i(m)$：投票者V_iの署名作成関数（ｍ：メッセージ）

$m=\zeta_i(s)$：投票者V_iの署名検証関数（ｓ：署名）

$s=\sigma_A(m)$：選挙管理者Ａの署名作成関数（ｍ：メッセージ）

$m=\zeta_A(s)$：選挙管理者Ａの署名検証関数（ｓ：署名）

$e=\omega_A(m,r)$：撹乱関数（ｍ：メッセージ、ｒ：乱数）

$y=\delta_A(d,r)$：乱数成分除去関数（ｄ：署名、ｒ：乱数）

ここで、選挙管理者の署名関数（δ_A，ζ_A）は、乱数による撹乱（ω_A）、および、乱数成分除去（δ_A）ができるものとする。

【００１１】

このような署名関数については、例えばＲＳＡ暗号の暗号化関数と復号化関数

があり（Ronald Rivest, Adi Shamir, Leonard Adleman：“A method for obtaining digital signatures and public-key cryptosystems”，Communications of the ACM, Vol.21, No.2, pp.120-126(Feb., 1978)），乱数による撹乱の手法についての詳細は、David Chaum：“Security without identification：Transaction systems to make big brother obsolete”，Communications of the ACM, Vol.28, No.10, pp.1030-1044(Oct., 1985)に記述されている。

【００１２】

以下、この発明の第一の実施例における投票の手順を示す。

Step 1　投票者V_iは、投票者装置１００により投票の準備を以下のように行う。

Step 1-1　投票者V_iは、投票内容v_iを暗号化器１１０で集計者Cの暗号化関数により暗号化し、投票用紙x_i

$$x_i = \xi_C (v_i)$$

を作成する。

【００１３】

Step 1-2　投票者V_iは、乱数生成器１２０を用いて乱数r_iを生成し、撹乱器１３０を用いてx_i、y_iを撹乱してe_i

$$e_i = \omega_A (x_i, r_i)$$

を作成する。

Step 1-3　投票者V_iは、署名作成器１４０を用いて、e_iの署名s_i

$$s_i = \sigma_i (e_i)$$

を作成し、$<e_i, s_i>$を選挙管理人Aの装置２００に送信する。

Step 2　選挙管理者Aは、選挙管理者装置２００により承認手続きを以下のように行う。

【００１４】

Step 2-1　選挙管理者Aは、投票者が有権者であることを、予め用意された有権者リストにあるか否かを投票権確認手段２１０により調べて確認する。もし、そうでなかったら、選挙管理者Aは承認を拒否する。

Step 2-2　選挙管理者Aは、これ以前に投票者V_iが選挙管理者Aによる承認

を受けているか否かを、投票者リストにV_iがあるかを投票権確認手段２１０により調べて検査する。もし、すでに承認されていたならば、選挙管理者Ａは二重投票として承認を拒否する。

【００１５】

Step 2-3　選挙管理者Ａは、署名検査器２２０を用いて、s_iとe_iを検査する。もし、合格ならば、選挙管理者Ａは、e_iを署名作成器２３０に通して、署名d_i

$$d_i = \sigma_A (e_i)$$

を計算し、d_iを投票者V_iの装置１００に送信する。これにより投票者V_iの承認を行う。また投票者リストに投票者V_iを追加する（投票者リストは投票開始時に予めすべて空白とされてある）。

【００１６】

Step 2-4　選挙管理者Ａは、投票者リストと投票者数を公表する。

Step 3　投票者V_iは、投票者装置１００により投票用紙とその署名情報を以下のように作成する。

Step 3-1　投票者V_iは、d_iとr_iを乱数成分除去器１５０に入力して、投票用紙x_iの署名情報y_i

$$y_i = \delta (d_i, r_i)$$

を求める。

【００１７】

Step 3-2　投票者V_iは、署名検査器１６０を用いて、y_iが選挙管理者Ａの署名であることを確認する。もし、不合格であったなら、投票者V_iは$<e_i, d_i>$を示すことにより、選挙管理者Ａの不正を主張する。

Step 3-3　投票者V_iは、前記署名確認が合格であれば$<x_i, y_i>$を集計者Ｃの装置３００に匿名通信路５００を用いて送信する。

Step 4　集計者Ｃは、集計者装置３００により以下のようにして票を収集する。

【００１８】

Step 4-1　集計者Ｃは、署名検査器３１０を用いてy_iが投票用紙x_iの署名であることを確認する。もし、合格ならば、集計者Ｃは投票リスト６０

０に、投票用紙x_iとその署名y_iを＜q，x_i，y_i＞と番号付けをして掲載する。

Step 4-2　すべての投票後、集計者Ｃはリスト６００を公表する（このリストはすべての投票者からアクセスが可能であるとする）。

Step 5　投票者V_iは、投票者装置１００により以下のようにして検証を行う。

【００１９】

Step 5-1　投票者V_iは、リスト６００に掲載された投票の数がStep 2-4で公表された投票者の数と一致するかを表検査器１７０で検査する。もし、不合格ならば、番号qと乱数r_iを公表して、選挙管理者Ａの不正を主張する。

Step 5-2　投票者V_iは、自らの投票用紙x_iが、リスト６００に掲載されているかを表検査器１７０で検査する。もし、掲載されていなければ、＜x_i，y_i＞を公表することにより、集計者Ｃの不正を主張する。

Step 6　集計者Ｃは、集計者装置３００により以下のようにして開票、および、集計を行う。

【００２０】

Step 6-1　投票者V_iからの投票用紙x_i、署名y_iの受信開始後、前記不正の通知が所定時間内になければ、集計者Ｃは、投票用紙x_iを復号化器３３０にて開票し、投票内容v_i

$$v_i = \rho_C(x_i)$$

を求め、投票内容v_iが正しい投票か、つまり投票内容v_iが正しいフォーマットになっているかを検査する。

【００２１】

Step 6-2　集計者Ｃは、投票内容v_iを集計器３４０を用いて集計し、その結果を周知するとともに、図１ｃに示すように、v_iをリストに追加する。

Step 7　投票者V_iは、投票者装置１００により集計者Ｃの操作が正しいことを確認する。つまり図１ｃに示すリスト中にすべてのv_iが追加されたか、また投票者V_iのx_iとv_iとが対応しているかを確認する。

【００２２】

以下では、この発明の第二の実施例について説明する。

これの全体構成は第一の実施例における集計者装置３００を分散集計者装置７００としたものと同じである。通信シーケンス例や投票者装置１００の構成例、選挙管理者装置３００の構成例などは集計者装置３００を分散集計者装置７００とする以外は先と同様である。以下、図６に分散集計者装置７００の構成例を示す。

【００２３】

ここで、分散集計者の暗号関数（ξ_C，ρ_C）は、それぞれの分散集計者が持つ鍵で復号化を行なうことで、暗号化された投票文が復号可能となったり、復号化に必要な人数にしきい値が存在し、一定数のしきい値付分散集計者が集まれば復号可能なようなものとする。

このような暗号関数については、例えばElGamal 暗号（Taher ElGamal ：“A public key cryptosystem and a signature scheme based on discrete logarithms ”，IEEE Transactions on Informatoin Theory, Vol.IT-31, No.4, pp.469-472(July, 1985)）の暗号化関数と復号化関数があり、これの分散した復号者による復号の手法やしきい値を導入した手法についての詳細は、Yvo Desmedt, Yale Frankel ：“Threshold cryptosystems ”in Advances in Cryptology-CRYPTO '89, Lecture Notes in Computer Science 435, Springer-Verlag, Berlin, pp. 307-315(1990) に記述されている。

【００２４】

以下、この発明の第二の実施例における投票の手順を示す。これは、第一の実施例のＳｔｅｐ６，７を以下のように変更したものであり、Ｋは分散集計者の人数である。

Step 6　分散集計者C_1,・・・，C_K は、分散集計者装置７００により、以下のようにして集計を行う。

【００２５】

Step 6-1　分散集計者C_1,・・・，C_K は、投票用紙x_i を分散復号化器７３０にて開票し、投票内容v_i を例えば次のようにして求める。

$x_{i1}=\rho_{C1}(x_i)$，$x_{i2}=\rho_{C2}(x_{i1})$，$x_{i3}=\rho_{C3}(x_{i2})$，・・・，$v_i=\rho_{CK}(x_{iK-1})$

求めた投票内容v_iが正しい投票かを検査する。

【００２６】

Step 6-2　分散集計者C_1,・・・，C_Kは、投票内容v_iを集計器７４０を用いて集計し、その結果を周知するとともに、v_iをリストに追加する。

Step 7　投票者V_iは、投票者装置１００により分散集計者C_jの操作が正しいことを確認する。

以下では、この発明の第三の実施例について説明する。

【００２７】

これの全体構成は第一の実施例における集計者装置３００をしきい値付分散集計者装置８００としたものと同じである。通信シーケンス例や投票者装置１００の構成例、選挙管理者装置３００の構成例などは集計者装置３００をしきい値付分散集計者装置８００とする以外は先と同様である。以下、図７にしきい値付分散集計者装置７００の構成例を示す。

【００２８】

以下、この発明の第三の実施例における投票の手順を示す。これは、第一の実施例のＳｔｅｐ６，７を以下のように変更したものであり、Ｋは分散集計者の人数、Ｌはしきい値である。

Step 6　しきい値付分散集計者C_1,・・・，C_Kは、しきい値付分散集計者装置８００により、以下のようにして集計を行う。

【００２９】

Step 6-1　しきい値付分散集計者C_1,・・・，C_Kは、投票用紙x_iをしきい値付分散復号化器８３０にて開票し、投票内容v_iを例えば次のように求める。分散集計者C_1,・・・，C_Kから任意に選んだＬ人の集計者をC_1,・・・，C_Lとし、しきい値付分散復号化器８３０により、

$x_{i1}=\rho_{C1}(x_i)$，$x_{i2}=\rho_{C2}(x_{i1})$，$x_{i3}=\rho_{C3}(x_{i2})$，・・・，$v_i=\rho_{CL}(x_{iL-1})$

を求め、投票v_iが正しい投票かを検査する。ここで、しきい値付分散

復号化器８３０はＬ個以上が作動すれば復号が可能であり、Ｌ未満であれば復号できないものとする。

【００３０】

Step 6-2　しきい値付分散集計者C_1,・・・, C_K は、投票内容v_iを集計器７４０を用いて集計し、その結果を周知するとともに、v_iをリストに追加する。

Step 7　投票者V_iは、投票者装置１００によりしきい値付分散集計者C_jの操作が正しいことを確認する。

【００３１】

ここで用いられた分散復号化器７３０としきい値付分散復号化器８３０は、例えば、上記のDesmedt-Frankel の方式を用いて構成されたものであり、例えば（しきい値）分散集計者C_1,・・・, C_K でそれぞれx_iを部分復号し、これらを１個所に集めてv_iを得るなど他の手法によってもよく、複数存在する（しきい値付）分散集計者間の通信等を必要とする場合がある。

【００３２】

図３乃至図７に示す各装置はその機能構成を示したものであり、これら各機能を動作を順次行わせるための制御手段を備え、また全体乃至一部をコンピュータにより実行させることもできる。

【００３３】

【発明の効果】

この発明では、投票内容（ｖ）を集計者の暗号化鍵で暗号化しているので、投票者は投票内容を復号化させるために、鍵を送信する必要がない。

続いて、集計者を複数とした場合には、集計者全員の合意が得られなければ開票作業が開始されない。

【００３４】

さらに、一定数の集計者が開票できる場合には、正当な集計者がある程度集まれば開票作業が開始でき、不正者もしくは故障者の影響を除去できる。

また、集計者が投票内容を改竄（かいざん）しても、公開された投票内容の一覧表を閲覧することで、投票内容の改竄を検出できる。すなわち、自らの投票が

利用されていないときには、暗号化された投票用紙x_iと選挙管理者の署名y_iを公開し、不正を主張すればよい。この際、不正な集計者の数が一定であるならば異議申し立て時のプライバシーは保証されている。

【００３５】

さらに、複数の集計者をおいた場合に、この発明では、暗号化鍵を用いて、投票内容を暗号化して送信しているので、投票用紙の収集の際に、集計者が途中経過を漏洩して選挙に影響を及ぼすといった不正が防止できる。

以上より、この発明では集計者の暗号化鍵を用いて、投票者の利便性を向上させ、また、集計者を複数とすることにより、途中経過を漏洩して選挙に影響を及ぼすといった不正を解決できる。

【図面の簡単な説明】

【図１】

ａはこの発明の全体構成を示すブロック図、ｂ，ｃはそれぞれ投票内容一覧表の例を示す図である。

【図２】

この発明方法の処理手順における通信シーケンスを示す図。

【図３】

投票者装置１００の機能構成例を示すブロック図。

【図４】

選挙管理者装置３００の機能構成例を示すブロック図。

【図５】

集計者装置４００の機能構成例を示すブロック図。

【図６】

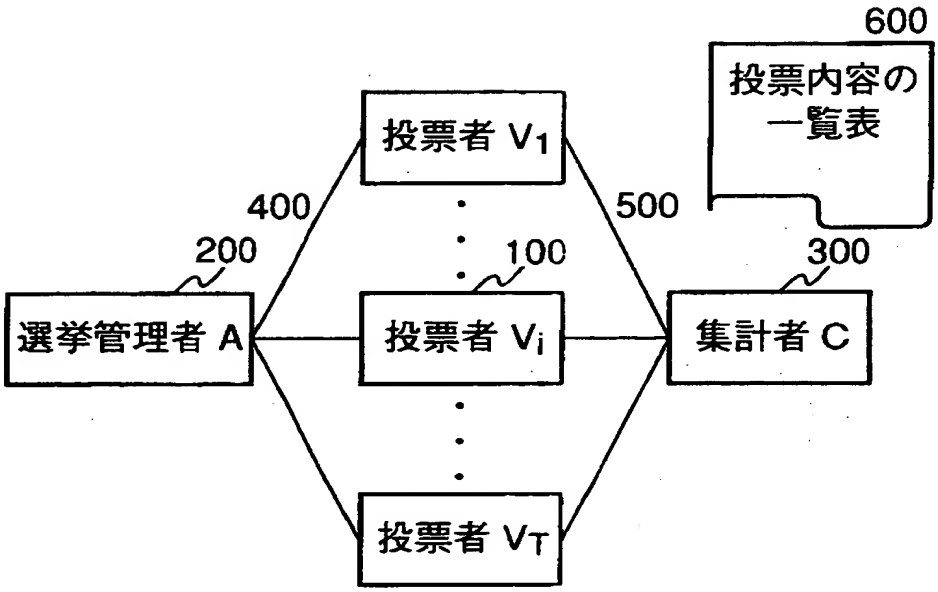
分散集計者装置７００の機能構成例を示すブロック図。

【図７】

しきい値付分散集計者装置８００の機能構成例を示すブロック図。

【書類名】　図面

【図１】



a

番号	投票内容（付加情報）
1	x_j,y_j
⋮	⋮
q	x_i,y_i
⋮	⋮

b

番号	投票内容（付加情報）
1	x_j,y_j,v_j
⋮	⋮
q	x_i,y_i,v_i
⋮	⋮

c

図　1

【図２】

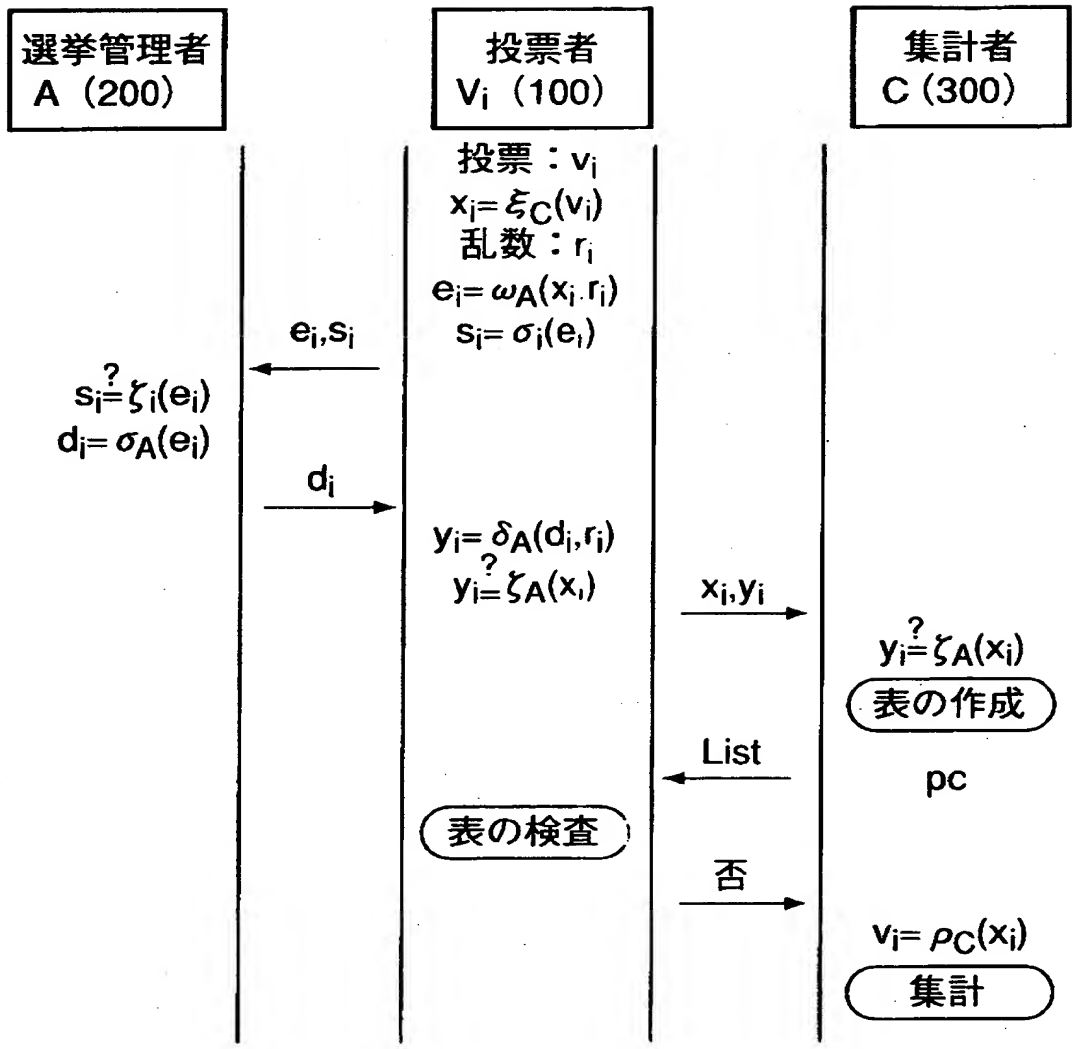

選挙管理者
A (200)
投票者
Vi (100)
集計者
C (300)
投票：vi
xi= ξC(vi)
乱数：ri
ei= ωA(xi, ri)
si= σi(ei)
ei,si
si?=ζi(ei)
di= σA(ei)
di
yi= δA(di,ri)
yi?=ζA(xi)
xi,yi
yi?=ζA(xi)
表の作成
List
pc
表の検査
否
vi= ρC(xi)
集計

図　２

【図３】

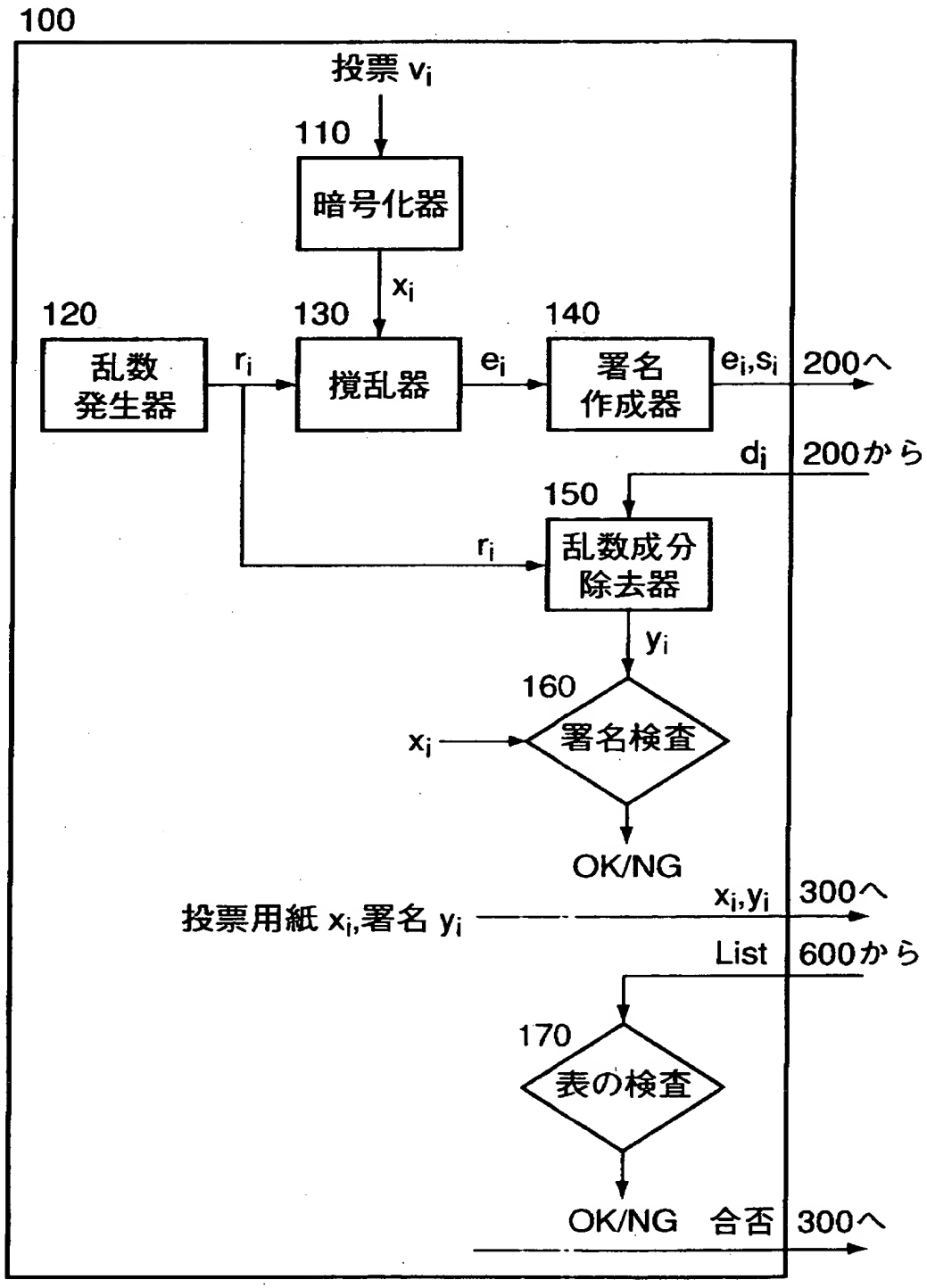

100
投票 v_i
110
暗号化器
x_i
120
乱数
発生器
r_i
130
撹乱器
e_i
140
署名
作成器
e_i,s_i
200へ
d_i
200から
150
乱数成分
除去器
r_i
y_i
160
署名検査
x_i
OK/NG
投票用紙 x_i,署名 y_i
x_i,y_i
300へ
List
600から
170
表の検査
OK/NG
合否
300へ

図　3

【図４】

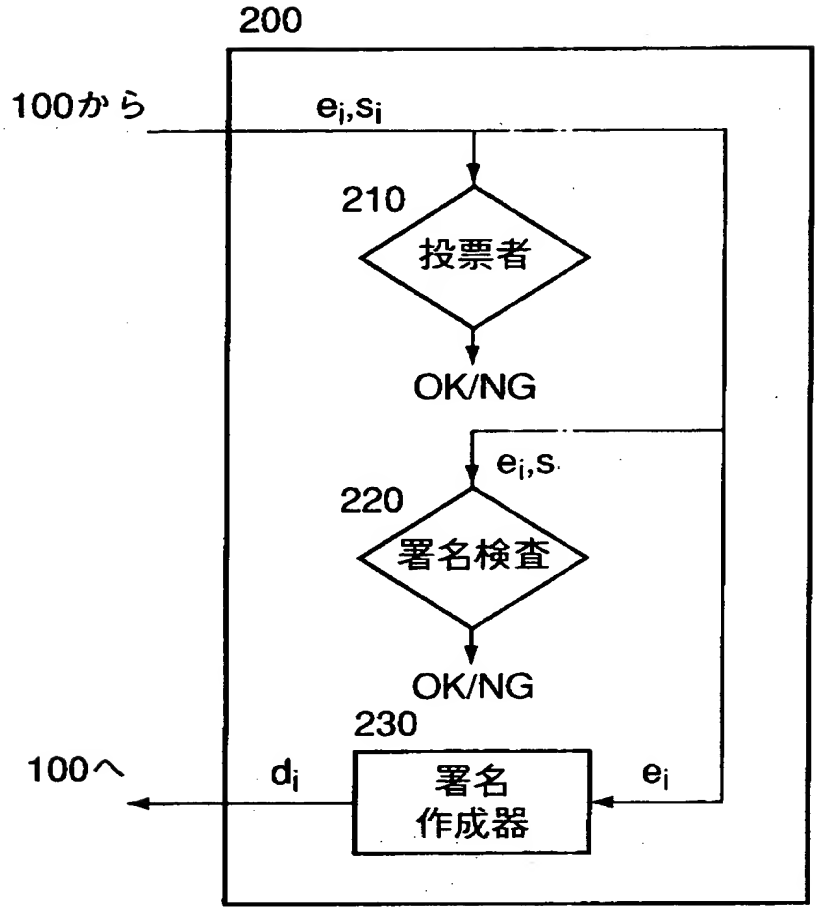

200
100から
e_i, s_i
210
投票者
OK/NG
e_i, s_i
220
署名検査
OK/NG
230
100へ
d_i
署名
作成器
e_i

図　4

【図５】

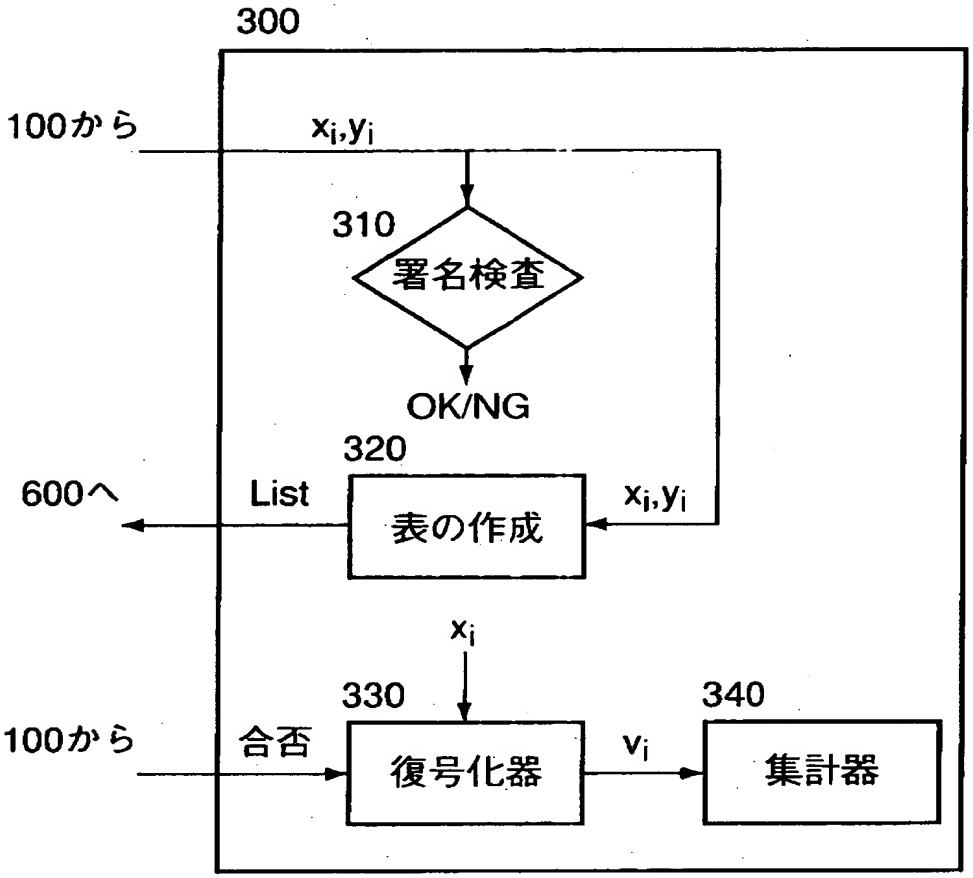

300
100から
x_i,y_i
310
署名検査
OK/NG
320
600へ
List
表の作成
x_i,y_i
x_i
330
340
100から
合否
復号化器
v_i
集計器

図　５

【図６】

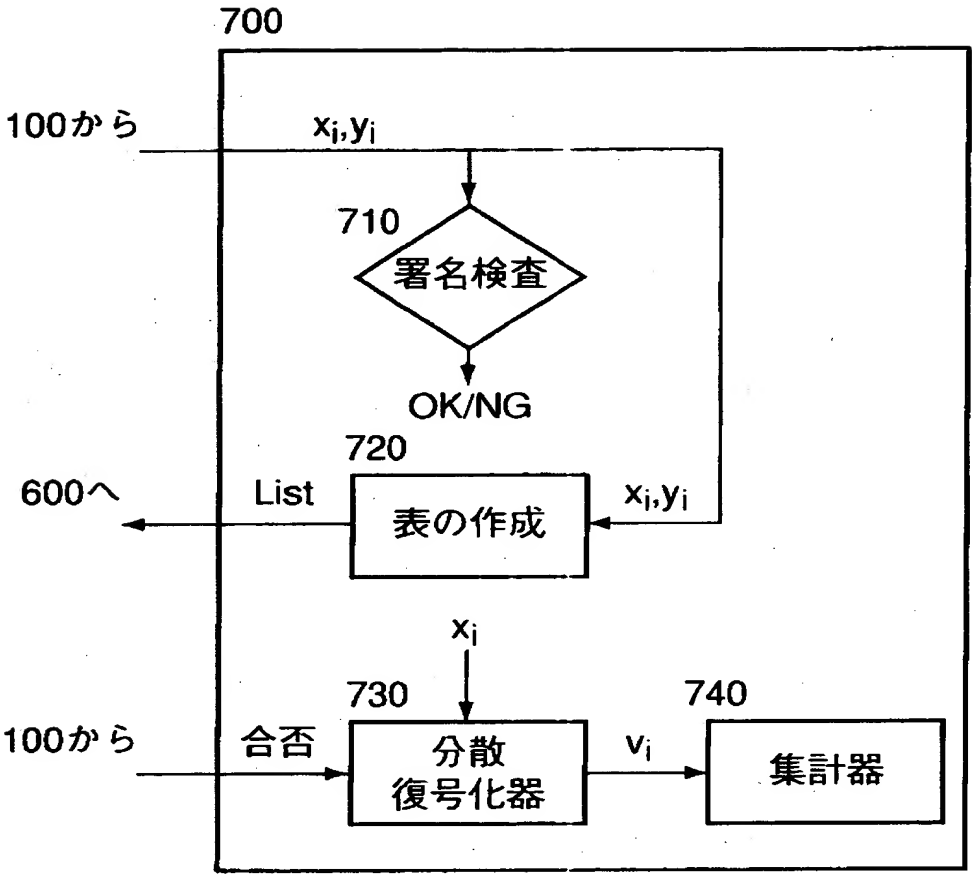

700
100から
x_i,y_i
710
署名検査
OK/NG
720
600へ
List
表の作成
x_i,y_i
x_i
730
740
100から
合否
分散
復号化器
v_i
集計器

図　6

【図７】

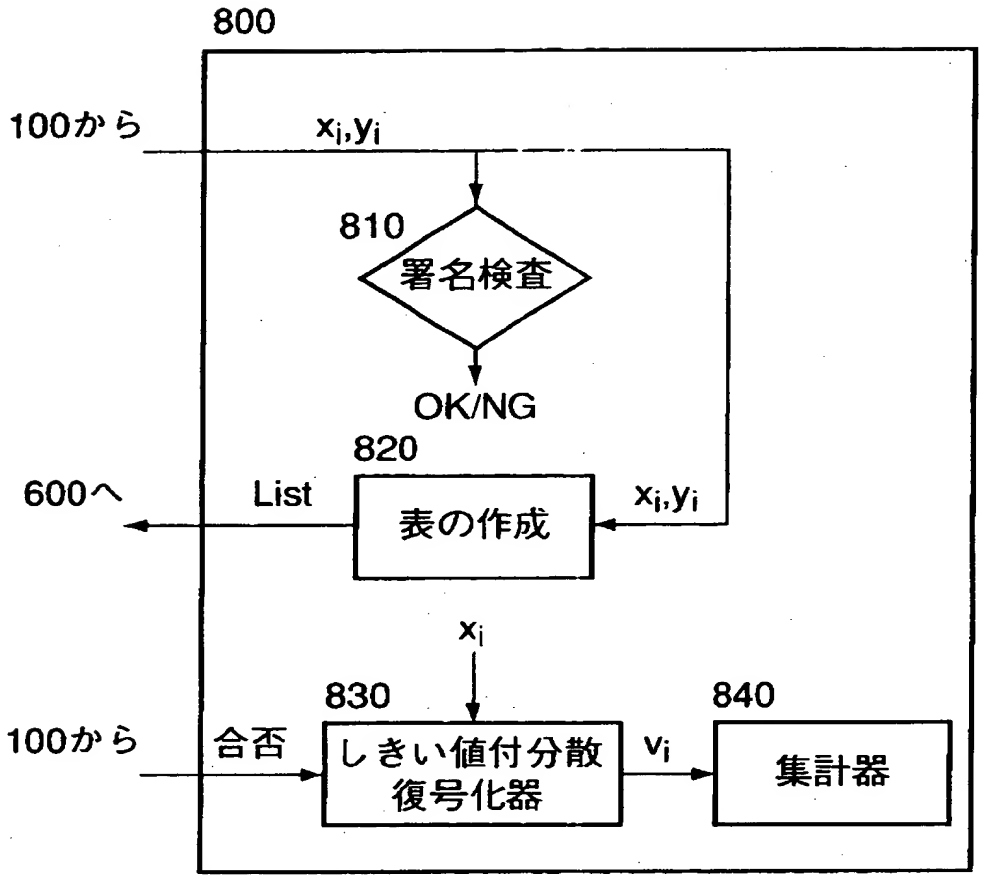

800
100から
x_i,y_i
810
署名検査
OK/NG
820
600へ
List
表の作成
x_i,y_i
x_i
830
840
100から
合否
しきい値付分散
復号化器
v_i
集計器

図　7

【書類名】　　要約書

【要約】

【課題】　投票者V_iは投票内容v_iを復号化させるために鍵を集計者Ｃへ送る必要がない。

【解決手段】　V_iはv_iをＣの鍵で暗号化し、その暗号化投票内容x_iを乱数r_iと共に撹乱して投票文e_iを作り、その署名s_iとe_iを選挙管理者Ａへ送り、Ａはe_iの署名d_iを作成してV_iへ返し、d_iからr_iの影響を除去した署名y_iを得、x_i，y_iをＣへ送り、Ｃでy_iを検証し、合格したらx_i，y_iの表を作り、公開し、V_iはその表を検査し、x_iがあることを確認し、Ｃはx_iを復号化してv_iを得、これを表に追加する。

【選択図】　　図２

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000004226
【住所又は居所】　東京都新宿区西新宿三丁目１９番２号
【氏名又は名称】　日本電信電話株式会社
【代理人】　申請人
【識別番号】　100066153
【住所又は居所】　東京都新宿区新宿四丁目２番２１号　相模ビル
【氏名又は名称】　草野　卓
【選任した代理人】
【識別番号】　100100642
【住所又は居所】　東京都新宿区新宿４丁目２番２１号　相模ビル　草野特許事務所
【氏名又は名称】　稲垣　稔

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９５年　９月２１日
［変更理由］　住所変更
住　所　東京都新宿区西新宿三丁目１９番２号
氏　名　日本電信電話株式会社

２．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社